Cassandra Crossing/ Lo smartphone è davvero spento?

(492)—od è un nemico in tasca? Dal bug "NoReboot" la prova della pericolosità dell'IoT.

Cassandra Crossing/ Lo smartphone è davvero spento?

Figure 1:

(492)—*od è un nemico in tasca? Dal bug "NoReboot" la prova della pericolosità dell'IoT.*

6 gennaio 2022—Come i 24 incanutiti lettori di Cassandra ricorderanno, le preoccupazioni della vostra profetessa preferita riguardo l'intrinseca pericolosità degli oggetti connessi risalgono all'ormai remoto 2006.
Si trattava allora della presenza di un "canale di ritorno" in un oggetto che doveva solo ricevere, e che inoltre poteva essere programmato da remoto via segnale televisivo si trattava dei rarissimi set-top box @MHP, rapidamente caduti nell'oblio delle tecnologie "nate morte", perché frutto solo di desideri di onnipotenza di alcune corporation, e non di reali necessità dei clienti.

Ma la preoccupazione di avere oggetti apparentemente "nostri" che in realtà eseguivano programmi per conto terzi e trasmettevano a loro i nostri dati personali era solo all'inizio.

In realtà il fatto di "non sapere" cosa faceva un oggetto era più pericoloso di usarlo sapendo esattamente quello che faceva.

Un sacco di anni sono passati, il mondo delle tecnologie è cambiato e l'IoT e gli smartphone sono tra noi.
La quasi totalità delle persone non si preoccupano minimamente di quanti e quali degli oggetti casalinghi od indossati siano controllati non da loro ma da enti terzi, e che questi oggetti trasmettano dati rilevati con una vasta quantità e tipologie di sensori.

Il “*computer pervasivo*”, una volta visto come benedizione, **ha ormai totalmente infiltrato la realtà**, mentre quasi tutti gli abitanti della parte digitalizzata di questo pianeta sono tranquilli e contenti.

Persino le recenti notizie sull’uso diffuso e sull’abuso dei software di intercettazione quali Galileo, FinFisher e NSO lasciano tranquilla la maggioranza degli utenti, che “*tanto non ho niente da nascondere*”.

Cassandra quindi, facendo il proprio mestiere, tenterà ancora di dare avvertimenti, instillando dubbi e paure salutari, come una volta si faceva con i bambini che volevano giocare con i fiammiferi.

Siete convinti che, se volete, potete spegnere il vostro smartphone, il vostro laptop, la vostra telecamera sorvegliapupo, il vostro braccialetto fitness, la vostra automobile, in modo da essere certi che non faccia nulla, che non ascolti, che non riferisca?

La risposta è si, ne siete convinti; infatti la maggior parte di questi oggetti alla fin fine hanno l’alimentazione elettrica, e quindi basta staccarla per renderli sordi ed inerti. Anche gli oggetti che vanno a batteria spesso permettono di rimuoverla, diventando anch’essi stessi certamente inerti.

Ma gli oggetti che contengono una batteria non rimovibile, ad esempio gli smartphone, possono comunque davvero essere spenti e resi inerti?

La risposta è no, purtroppo anche no. Se un oggetto viene fatto funzionare da un software, anche se lo spegnimento e l’accensione sono governati da un “pulsante di spegnimento”, questo non è un “interruttore elettrico”. Il pulsante si limita ad eseguire un software, che “dovrebbe” spegnere l’oggetto.

E del software non ci si può fidare.

E’ già pericoloso quando è inutilmente complesso e quindi scritto male, ma diventa un’arma tanto impercettibile quanto inarrestabile quando è scritto con malizia.

Siete convinti di poter spegnere il vostro smartphone ultrasicuro?

Magari una della famiglia degli iCosi?

Bene, la risposta è che vi sbagliate.

Questo articolo “*Persistence without ”Persistence”: meet The Ultimate Persistence Bug, NoReboot*” che riguarda per ora solo i possessori di smartphone Apple, dettaglia come si può sovvertire iOS per “mimare” le procedure di spegnimento e riaccensione, in modo da lasciare il cellulare apparentemente “spento”, ma in realtà in pieno funzionamento, rete, wifi e bluetooth compresi.

E poter, di conseguenza, farlo agire come device di sorveglianza, anche in situazioni apparentemente estremamente private.

Poco altro resta da dire. Chiudiamo semplicemente come fa l’autore dell’interessantissimo articolo.

“***Mai essere sicuri che un device sia spento***”

sponsorizzando anche il suo consiglio di “***Controllate che il vostro device non sia compromesso***”.

La “compromissione” pericolosa infatti non è quella di una eventuale installazione di un captatore informatico, come quello di NSO, ma quella fatta “by design” dal costruttore, che esiste sempre e sta diventando la regola.

Troppa paranoia? Magari!

Almeno i paranoici di oggi non scoprirebbero, tra dieci anni, di essere stati ancora una volta degli inguaribili ottimisti.

By Marco A. L. Calamari on January 6, 2022.

Canonical link

Exported from Medium on August 27, 2025.